

# Uso adecuado de las redes sociales





- ▶ Las **redes sociales** se han hecho un lugar muy fuerte en nuestras vidas por lo que debemos hacer un buen **uso de las redes sociales** para proteger nuestra privacidad.

# 8 consejos para evitar correr riesgos en las redes sociales

- ▶ **1. Lo primero un buen antivirus.** Tener instalada la última versión de tus aplicaciones y sistema operativo es el primer paso de seguridad. El segundo es evitar la infección de virus (software que se instala en tu ordenador sin tu consentimiento y cuyo propósito es dañar su funcionamiento y actuar de transmisor para dañar otros ordenadores, generalmente mediante el e-mail) con un antivirus.
- ▶ **2. No caigas en el phishing.** Las cadenas de mensajes (correos que te invitan a reenviarse con un contenido atractivo) y los mails que te avisan de un supuesto problema solicitándote que accedas a una página web (donde tendrás que proporcionar tu usuario y contraseña) son la mejor forma de facilitar la infección de virus y de que se capturen tus credenciales, respectivamente. Ninguna entidad bancaria ni organización alguna envía correos electrónicos solicitando datos de acceso, así que desconfía de todo ese tipo de mensajes. Nunca abras archivos adjuntos que recibas en tu cuenta de e-mail, si desconoces el remitente y, aunque lo conozcas, no lo abras si no lo solicitaste

- ▶ **3. Supervisa la actividad de tus hijos menores de edad en la Red.** Tener el ordenador (computador) en un lugar común del hogar.
- ▶ **4. Configura una buena contraseña y activa el acceso en dos pasos.** Tu contraseña es la llave de oro a tus actividades en la Red. Una contraseña es relativamente fácil de averiguar con técnicas de ingeniería social y phishing. Pero existen métodos para combatirlas: establece contraseñas fuertes; es decir, contraseñas que contengan al menos 8 caracteres incluidas mayúsculas, minúsculas, símbolos y números. Algunas aplicaciones, como Google y Dropbox, permiten la verificación en dos pasos (uso del teléfono móvil para recibir un código que te permite completar el login). Activa esa opción siempre que sea posible.

- ▶ **5. Configura los parámetros de privacidad.** Todas las redes sociales incorporan opciones de privacidad para configurarlas a tu gusto. Tú decides quién accede a tus contenidos y cómo. Revisálas bien antes de publicar nada. Es preferible organizar a tus contactos por listas o categorías y ofrecerles contenidos con distintos niveles de privacidad.
- ▶ **6. No aceptes relaciones con desconocidos.** Con toda seguridad, una gran parte de los contactos de una red social no son tus amigos de verdad. Aprende a diferenciar los matices del concepto de “seguidor” y “amigo” en la Red. En Twitter, tus seguidores son tu audiencia, la gente que lee tus publicaciones. Y tú sigues a usuarios que te interesan por lo que aportan. No es necesario que ninguno de ellos sea tu amigo realmente. En Facebook, sin embargo, solo deberías agregar a personas que conozcas y que te inspiren confianza.

- ▶ **7. No publiques información comprometida.** Ni en Twitter ni en Facebook, o similares, proporcionas datos que permitan a otros ubicar tu domicilio, escuela, lugar de trabajo, etc.
- ▶ **8. Si hay sospechas de delito denúncialo.** Como ves, tú posees el control de lo que publicas en Internet y de lo que otros puedan publicar en tu perfil en aplicaciones como Facebook. Sin embargo, ¿qué sucede con lo que se publica en sitios que tú no gestionas?. ¿Y si alguien me fotografía sin mi permiso y lo cuelga en la Red? Ese es un temor muy común y comprensible. Sin embargo, todas las redes sociales poseen opciones de denuncia de abusos y contenido inapropiado. Con toda seguridad el contenido será retirado rápidamente.

# PAPÁS PARA TENER EN CUENTA

Algunas formas para ayudar a los hijos a usar los sitios de redes sociales de forma más segura

- ▶ **Hable con sus hijos sobre sus experiencias.** Incentive a sus hijos a que le cuenten si algo que encuentran en uno de estos sitios los hace sentir preocupados, incómodos o amenazados. Mantenga la calma y hágales saber que no se meterán en problemas por avisarle si pasa algo. Hágales saber que los ayudará a resolver la situación para que ésta tenga un resultado positivo.
- ▶ **Establezca sus propias reglas sobre Internet en su hogar.** Cuando sus hijos comiencen a usar Internet solos, es aconsejable confeccionar una lista de reglas para el uso de Internet con la que todos estén de acuerdo. Esas reglas deben incluir si sus hijos pueden usar sitios de redes sociales y cómo pueden usarlos. Para obtener más información sobre cómo establecer reglas, consulte [Uso de contratos familiares para proteger a los niños cuando están en línea](#).

- ▶ **Asegúrese que sus hijos respeten los límites de edad del sitio que visitan.** En general, la edad recomendada para unirse a una red social es 13 años o más. Si sus hijos tienen menos de la edad recomendada para estos sitios, no los deje usarlos. Es importante que recuerde que no puede confiar en que los servicios de Internet evitarán que su hijo se una a la red porque no cuenta con la edad recomendada.
- ▶ **Aprenda sobre el sitio.** Evalúe los sitios que sus hijos planean visitar y asegúrese de que tanto usted como sus hijos comprendan las políticas de privacidad y el código de conducta de cada sitio. Averigüe si el sitio controla el contenido que se publica en él. Asimismo, revise la página de sus hijos de forma periódica. Para obtener más consejos, consulte Sugerencias para padres e hijos sobre el uso seguro de blogs.

- ▶ **Insista en que sus hijos no se encuentren en persona con alguien que conocen sólo en línea y alíentelos a que se comuniquen solamente con gente que conocen en persona.** Es realmente peligroso que un niño se encuentre con personas que sólo conoce por Internet. Puede contribuir a proteger a sus hijos si los alienta a que usen estos sitios para comunicarse con sus amigos, no para comunicarse con gente que nunca han conocido en persona.
- ▶ **Asegúrese de que su hijo no use su nombre completo.** Dígale a sus hijos que usen solamente sus primeros nombres o un alias que no atraiga atención inadecuada. Asimismo, no permita que sus hijos publiquen los nombres completos de sus amigos.

- ▶ **Tenga cuidado con los detalles que aparecen en las fotografías.** Explique a sus hijos que las fotografías pueden revelar mucha información personal. Hable con sus hijos para que no publiquen fotografías de ellos o de sus amigos que contengan detalles de fácil identificación como por ejemplo señales que se encuentran en la calle, el número de matrícula de su auto o el nombre de su escuela escrito en los buzos que llevan **puestos**.
- ▶ **Hábleles a sus hijos acerca del ciberacoso.** Cuando sus hijos tengan edad suficiente para usar sitios de redes sociales, hable con ellos sobre el ciberacoso. Hágalos saber que, si creen ser víctimas de ciberacoso, deben acudir inmediatamente a sus padres, a su profesor o a otro adulto de confianza. Es también importante alentar a sus hijos a que se comuniquen con otros en línea del mismo modo que lo harían personalmente. Indíqueles que deben tratar a los demás como a ellos les gustaría ser tratados.



# Videos de apoyo

- ▶ <https://youtu.be/1VAL7lFGSD4>
- ▶ <https://www.youtube.com/watch?v=Ak3qp4qRAiY>

# Bibliografía

- ▶ <https://www.frikipandi.com/internet/20121029/8-recomendaciones-para-evitar-correr-riesgos-en-redes-sociales/>